May 27, 2016

North Dakota State and Local Intelligence Center

Bi-Weekly Cyber Rollup

Included in this week's summary:
Click on the Section Header to go directly to that location in the Summary

NORTH DAKOTA & REGIONAL
(U) Ransomware discovered on state of North Dakota server and laptop
(U) Two North Dakota entities experienced ACH fraud

NATIONAL
(U) Skimmers found at Walmart
(U) Serious vulnerabilities found in Moxa industrial secure routers
(U) Hackers Spying on US Presidential Campaigns

INTERNATIONAL
(U) Water treatment plant hacked, chemical mix changed for tap supplies
(U) Data leaked from hacker forum Nulled.io
(U) Researchers crack new version of CryptXXX ransomware.
(U) Five-year-old SAP vulnerability affects over 500 companies, not 36
(U) Critical vulnerability in Symantec AV Engine exploited by just sending an email.

NORTH DAKOTA & REGIONAL

(U) Ransomware discovered on state of North Dakota server and laptop

(U) State of North Dakota discovered ransomware on a server and laptop. The malware discovered was "locky" ransomware which behaves like most other ransomware, encrypting files and holding them for ransom, asking you to pay to unlock the files: https://blog.malwarebytes.org/threat-analysis/2016/03/look-into-locky/

Source of the infection was found, both server and workstation were taken offline. In total the ransomware was active roughly 20 minutes and encrypted 9000+ files. We believe the ransomware was obtained by downloading a zip file from a personal webmail account.

Images of the server and workstation hard drives were sent to MS-ISAC for further forensics. The server was restored and workstation rebuilt.

(U) Two North Dakota entities experienced ACH fraud

(U) Two North Dakota entities experienced ACH fraud in the past two weeks. One entity experienced two fraudulent transactions: an online payment to Bloomingdales for over $15,000 and a Discover epayment ACH DB for $1426. They view their accounts daily and caught it right away. The other entity experienced several online transactions throughout a three week period to vendors such as Bloomingdales, Zales, and others. The transactions total over $96,000. Because the transactions were caught in a timely manner, the entities did not lose funds.

All fraudsters need is the routing and account number (which is on checks that are issued) to make an online payment. Check your bank accounts on a daily basis.

NATIONAL

(U) Skimmers found at Walmart

(U) Found in self-checkout lanes at some Walmart locations were credit card skimmer devices.

The skimmers were made to piggyback on card readers. This device includes an overlay to capture a user's PIN and a mechanism for recording the data stored on a card's magnetic stripe.

This particular skimmer retails for between $200 to $300, but that price doesn't include the electronics that power the device and store the stolen card data.

http://krebsonsecurity.com/2016/05/skimmers-found-at-walmart-a-closer-look/

(U) Hackers Spying on US Presidential Campaigns

(U) The United States sees evidence of hackers, possibly working for foreign governments, snooping on the presidential candidates, the nation's intelligence chief said Wednesday. Government officials are assisting the campaigns to tighten security as the race for the White House intensifies.

http://gadgets.ndtv.com/internet/news/hackers-spying-on-us-presidential-campaigns-official-839479

(U) Serious vulnerabilities found in Moxa industrial secure routers.

(U) Moxa released a firmware update for its EDR-G903 series industrial routers versions 3.4.11 and older, patching several high severity vulnerabilities that can be exploited for denial-of-service (DoS) attacks, privilege escalation, and arbitrary code execution, including configuration and log files that can be accessed on the Web server by accessing a specific Uniform Resource Locator (URL), allowing an unauthenticated attacker to download the configuration and log files.

http://www.securityweek.com/serious-vulnerabilities-found-moxa-industrial-secure-routers

INTERNATIONAL

(U) Water Treatment plant hacked, chemical mix changed for tap supplies

(U) Hackers infiltrated a water utility's control system and changed the levels of chemicals being used to treat tap water. Cyber-attack is document in March's IT security breach report from Verizon Security Solutions.

The hack involved SQL injection and phishing.

http://www.theregister.co.uk/2016/03/24/water_utility_hacked/

(U) Data leaked from hacker forum Nulled.io.

(U) Risk Based Security reported that the popular forum, Nulled.io was compromised after hackers leaked a 1.3Gb archive containing more than 536,000 user account information including usernames, email addresses, hashed passwords, application program interface (API) credentials for payment gateways, authentication logs, and Internet Protocol (IP) addresses, among other data. Researchers are unsure how the Nulled.io database was compromised and the forum was taken offline due to the attack.

http://www.securityweek.com/data-leaked-hacker-forum-nulledio

(U) Researchers crack new version of CryptXXX ransomware.

(U) Researchers from Kaspersky Lab created a new tool titled, RannohDecryptor that will help victims decrypt files and recover lost information affected by the CryptXXX 2.0 malware. Researchers advised users to install software program updates to mitigate ransomware attacks.

http://www.networkworld.com/article/3070477/researchers-crack-new-version-of-cryptxxx-ransomware.html

(U) Five-year-old SAP vulnerability affects over 500 companies

(U) The U.S. Computer Emergency Response Team (US-CERT) issued a public alert to all U.S. companies after ERPScan discovered at least 533 companies were affected by an SAP vulnerability largely due to the companies' failure in installing a SAP security patch issued in 2010. The vulnerability can allow attackers to gain complete control of SAP business platforms via a bug in Invoker Servlet, a component in SAP's Java platforms.

http://news.softpedia.com/news/five-year-old-sap-vulnerability-affects-over-500-companies-not-36-504043.shtml

(U) Critical vulnerability in Symantec AV Engine exploited by just sending an email.

(U) Symantec updated its Antivirus Engine (AVE) addressing a critical memory corruption flaw after a security researcher from Google Project Zero discovered the flaw affected most Symantec and Norton-branded antivirus products and reported the issue related to how the antivirus products handle executables compressed in the ASPack file compressor. The vulnerability can be remotely exploited for code execution by sending a specially crafted file to the victim.

http://www.securityweek.com/critical-vulnerability-symantec-av-engine-can-be-exploited-sending-email